Universidad Americana de Europa UNADE

Doctorado en Informática

Modelo de Madurez de Capacidades de Ciberseguridad para Instituciones de Educación Superior Colombianas MMCC-IES

Diagnóstico empírico: n=129 actores · 5 instrumentos · Marzo - Mayo 2026

Caso piloto: Universidad Nacional Abierta y a Distancia – UNAD

TLP:CLEAR **:** Se usa cuando la información no genera ningún riesgo de mal uso y pueda ser difundido de forma pública. En este sentido, la información puede ser distribuida sin restricciones, pero sujeta a controles de derechos de autor

MMCC-IES

Medio de divulgación:
Correo Electrónico - Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Edición electrónica

Doctorado en Informática

Doctorando
Luis Fernando Zambrano Hernández

Directora
Rosa Gabriela Camero

Panel de Validación - Coeficiente V de Aiken

Ing Andrés Ernesto Salinas Duarte
Ing. Hernando José Peña Hidalgo
Ing. Sonia Ximena Moreno Molano
Ing Cesar Villamizar
Ing Daniel palomo Luna
Ing Nestor Cardenas Corral
Ing Victor Manuel Zambrano Hernandez
Adm. Libardo Cardenas Corral

Contenido

1. INTRODUCCIÓN GENERAL AL MODELO MMCC-IES 5
1.1. Arquitectura del Modelo 6
2. LOS CINCO NIVELES DE MADUREZ DEL MMCC-IES 7
2.1. Sistema de Codificación de Indicadores 7
3. DIMENSIÓN 1: GOBERNANZA INSTITUCIONAL DE CIBERSEGURIDAD 8
3.1. Fundamento y Justificación 8
3.2. Indicadores Detallados por Nivel 9
Nivel 1 - Reactivo: Sin gobernanza formal 9
Nivel 2 - Emergente: Política básica sin seguimiento 10
Nivel 3 - Estructurado: CISO formal y comité activo 10
Nivel 4 - Gestionado: Integración estratégica plena 11
Nivel 5 - Resiliente: Gobernanza adaptativa de IA 11
3.3. Indicadores - Dimensión Gobernanza 12
4. DIMENSIÓN 2: TALENTO HUMANO Y COMPETENCIAS K-S-A 13
4.1. Fundamento y Justificación 13
4.2. Indicadores Detallados por Nivel 14
Nivel 1 - Reactivo: Sin roles definidos 14
Nivel 2 - Emergente: Roles básicos informales 14
Nivel 3 - Estructurado: Equipo o Equipos con perfiles NICE 15
Nivel 4 - Gestionado: Formación continua medida 15
Nivel 5 - Resiliente: Especialistas en IA y redes CSIRT internacionales 16
4.3. Indicadores: Dimensión Talento Humano 17
5. DIMENSIÓN 3: GESTIÓN DE RIESGOS DE CIBERSEGURIDAD 18
5.1. Fundamento y Justificación 18
5.2. Indicadores Detallados por Nivel 19
Nivel 1 - Reactivo: Sin inventario de activos 19
Nivel 2 - Emergente: Inventario básico y análisis ad hoc 19
Nivel 3 - Estructurado: Metodología formal periódica 20
Nivel 4 - Gestionado: Riesgos en las decisiones de inversión TI 20
Nivel 5 - Resiliente: Gestión predictiva con threat intelligence 21
5.3. Indicadores - Dimensión Gestión de Riesgos 22
6. DIMENSIÓN 4: CAPACIDADES TÉCNICAS DE CIBERSEGURIDAD 23
6.1. Fundamento y Justificación 23

6.2. Indicadores Detallados por Nivel 24
Nivel 1 - Reactivo: Controles básicos aislados 24
Nivel 2 - Emergente: Controles básicos implementados 24
Nivel 3 - Estructurado: SIEM, MFA e IR probado 25
Nivel 4 - Gestionado: SOC 24/7, BCP/DRP probado y hardening sistemático 25
Nivel 5 - Resiliente: XDR, Zero Trust pleno y threat hunting proactivo 26
6.3. Indicadores - Dimensión Capacidades Técnicas 26
7. DIMENSIÓN 5: SEGURIDAD DE INTELIGENCIA ARTIFICIAL (ISO 42001:2023) . 28
7.1. Fundamento y Justificación: La Dimensión Diferenciadora 28
7.2. Indicadores Detallados por Nivel 29
Nivel 1 - Reactivo: Sin política de IA - Opacidad total 29
Nivel 2 - Emergente: Política básica e inventario inicial 30
Nivel 3 - Estructurado: SGIA activo con los cuatro ejes operativos 31
Nivel 4 - Gestionado: SGIA auditado y XAI plena 32
Nivel 5 - Resiliente: SGIA certificado y gestión total del ecosistema 33
7.3. Indicadores - Dimensión Seguridad de IA 34
8. CULTURA ORGANIZACIONAL DE SEGURIDAD: VARIABLE MODERADORA TRANSVERSAL 35
8.1. Función Moderadora en el Modelo 35
8.2. Criterios de Cultura por Nivel 35
9. POSICIONAMIENTO DIAGNÓSTICO DE LA UNAD EN EL MODELO MMCC-IES 37
10. RUTAS EVOLUTIVAS INSTITUCIONALES ESCALABLES 39
11. REFERENCIAS BIBLIOGRÁFICAS 41

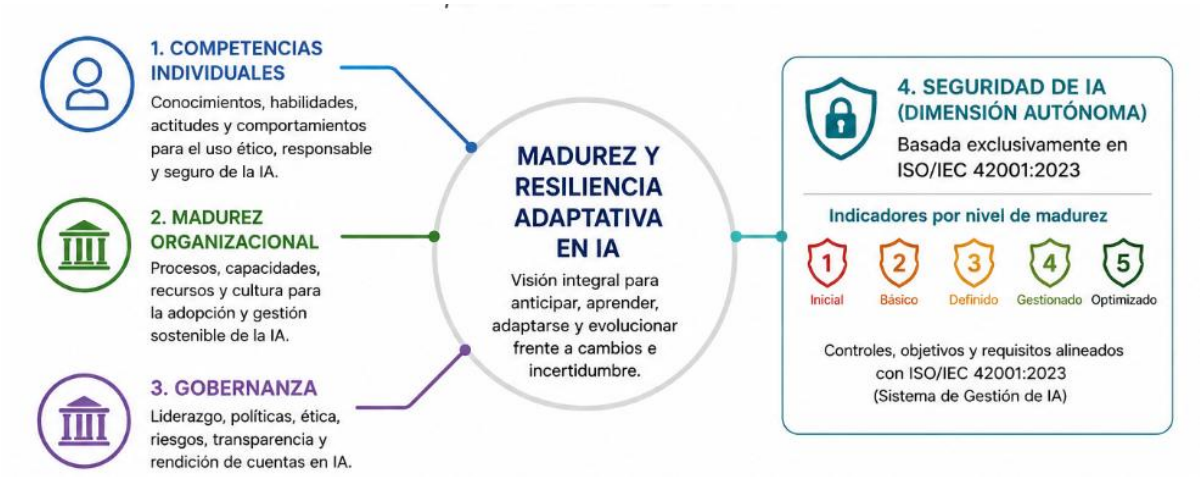
1. INTRODUCCIÓN GENERAL AL MODELO MMCC-IES

El Modelo de Madurez de Capacidades de Ciberseguridad para Instituciones de Educación Superior Colombianas MMCC-IES, es la contribución original de esta investigación doctoral al campo del conocimiento. Integra de forma sistemática los resultados del Objetivo específico 1 (RSL con 96 estudios, seis marcos normativos, cuatro vacíos identificados) y del Objetivo Especifico 2 (diagnóstico empírico con 129 actores de cinco grupos diferenciados, cinco instrumentos, cinco hallazgos de alta convergencia) en una arquitectura evaluativa operacional para el contexto universitario colombiano. No es una adaptación de marcos existentes.

La Teoría de Capacidades Dinámicas (Teece et al., 1997) provee el fundamento epistemológico. Los cinco niveles del modelo no son estados estáticos de cumplimiento sino trayectorias de evolución adaptativa que operan en tres procesos: sensing (detección de señales del entorno de amenazas), seizing (formulación y captura de respuestas estratégicas) y transforming (reconfiguración continua de capacidades ante cambios tecnológicos o regulatorios). El Nivel 5 (Resiliente), corresponde a organizaciones con capacidad plena de transforming.

El modelo tiene cuatro diferenciadores respecto a los marcos existentes (CMM/GCSCC, NIST CSF 2.0, NICE, ECSF):

Ilustración 1.
Fases del MMCC-IES



Elaboración propia apoyada por IA

1.1. Arquitectura del Modelo

El MMCC-IES se organiza en cinco dimensiones evaluadas en cinco niveles, con la Cultura Organizacional como variable moderadora transversal. Total: 83 indicadores codificados como **I[Nivel].[Dimensión].[Número]**.

Ilustración 2.
Arquitectura del modelo MMCC-IES

DIMENSIÓN	Reactivo	Emergente	Estructurado	Gestionado	Resiliente
Gobernanza	Sin política formal. Sin CISO. Sin presupuesto propio.	Política básica aprobada. Responsable TI sin mandato.	CISO formal con KPIs. Comité directivo activo.	Alineación estratégica plena en el PDI.	Gobernanza ética IA. Vigilancia regulatoria activa.
Talento Humano	Sin roles formales. Sin plan de formación.	Roles básicos. Formación esporádica.	Equipos NICE/ECSF. Articulación académica.	Certificaciones medidas. Brechas K-S-A evaluadas.	Especialistas IA. Red Team sistemático.
Gestión de Riesgos	Sin inventario. Sin evaluaciones formales.	Inventario básico. Análisis ad hoc.	Metodología formal periódica. Plan de tratamiento.	Riesgos en decisiones TI. Tiempos REDSIIUNAD.	Threat intelligence. Modelos predictivos de amenazas.
Cap. Técnicas	Controles básicos aislados. Sin IR plan.	Firewall, AV, backups básicos.	SIEM operativo. MFA. IR probado.	SOC 24/7. Zero Trust. BCP/DRP verificado.	XDR/MDR con ML. Threat hunting proactivo.
Seguridad IA ★	Sin política IA. Shadow AI libre. Opacidad total.	Política básica. Inventario IA. Transparencia inicial.	AIIA. Control de sesgos. Ecosistema IA controlado.	AIMS auditado. XAI plena. Cadena suministro IA.	ISO 42001 certificado. EU AI Act. Gestión total.
Cultura Organizacional de Seguridad — Variable moderadora transversal presente en todos los niveles como condición de sostenibilidad					

Nota. *Ilustración 2. Arquitectura del Modelo MMCC-IES. Total: 83 indicadores. Dimensión diferenciadora respecto a todos los modelos de referencia existentes. Elaboración propia basada en recopilación de información a partes interesadas.*

2. LOS CINCO NIVELES DE MADUREZ DEL MMCC-IES

Los cinco niveles del MMCC-IES tienen nombres propios que capturan el comportamiento organizacional dominante en cada circuito con mayor precisión que los modelos precedentes. El nombre del nivel máximo (Resiliente) ancla el horizonte del modelo en el paradigma de resiliencia adaptativa coherente con el NIST CSF 2.0 Tier 4 y con la Teoría de Capacidades Dinámicas.

Tabla 1.
Niveles de madurez del MMCC-IES

N	Nombre	Comportamiento dominante	Capacidad dinámica
1	Reactivo	Sin anticipación ni prevención. Responde únicamente a incidentes ya materializados. Sin política, sin CISO, sin presupuesto propio.	Sin sensing: no detecta señales del entorno de amenazas.
2	Emergente	Primeros controles y políticas sin coherencia sistémica ni seguimiento. Función de seguridad sin capacidad institucional estructurada.	Sensing incipiente: identifica amenazas sin mecanismo formal de respuesta.
3	Estructurado	Procesos formalizados, responsabilidades asignadas, herramientas básicas operativas. Posible coexistencia de capacidades técnicas sólidas con brechas de gobernanza.	Seizing parcial: respuesta operativa pero no integración estratégica plena.
4	Gestionado	Ciberseguridad integrada en la planeación estratégica con indicadores cuantitativos. La distinción crítica con N3: la integración estratégica, no la sofisticación técnica.	Seizing pleno: integra la ciberseguridad en decisiones estratégicas y presupuestales.
5	Resiliente	Anticipa, aprende y se adapta de forma continua. Gobernanza de IA integrada. Vigilancia regulatoria activa. ISO 42001:2023 en proceso o alcanzada.	Transforming pleno: reconfigura capacidades ante cambios tecnológicos y regulatorios del entorno.

Nota. *Tabla 1. Los cinco niveles del MMCC-IES con comportamiento dominante, capacidad dinámica* (Teece et al., 1997). *Fuente: partes interesadas consultadas (n=129, 2026). Elaboración propia.*

2.1. Sistema de Codificación de Indicadores

Todos los indicadores siguen la codificación I[Nivel].[Dimensión].[Número]. El Nivel va de 1 a 5; la Dimensión se identifica como G (Gobernanza), T (Talento Humano), R (Gestión de Riesgos), C (Capacidades Técnicas) o IA (Seguridad de IA); el Número identifica el indicador dentro de la celda. Ejemplo: I3.IA.2 = Nivel 3, Dimensión Seguridad de IA, indicador 2 (evaluación de sesgos por grupos protegidos).

3. DIMENSIÓN 1: GOBERNANZA INSTITUCIONAL DE CIBERSEGURIDAD

Código: D1-GOB · **Indicadores:** 8 (I1.G.1 a I5.G.2) ·

Respaldo empírico: 63,5% - 92,3% consenso transversal

Referentes: (National Institute of Standards and Technology, 2024b) · ((Gcscc), 2021) · ISO 27001:2022 Cláusula 5 · (Cheng & Wang, 2022)

3.1. Fundamento y Justificación

La gobernanza es la dimensión de mayor consenso transversal: entre el 63,5% y el 92,3% de los actores consultados la identifica como dimensión prioritaria según el grupo. El (National Institute of Standards and Technology, 2024a) la reconoce como el eje que condiciona todas las demás funciones de ciberseguridad mediante la función Govern, novedad relevante respecto al CSF 1.1. Tres desafíos estructurales documentados en las IES colombianas:

- Fragmentación de responsabilidades entre TI, dependencias y comités de riesgo
- Ausencia de CISO con mandato formal que le permita imponer controles sobre otras áreas
- Desalineación presupuestal que convierte la ciberseguridad en gasto contingente a incidentes en lugar de inversión estratégica planificada.

La paradoja técnico gobernanza de la UNAD, equipo técnico alto - muy alto en el 85,7% pero preparación moderada para incidentes complejos en el 78,6%, es consecuencia directa de la ausencia de integración estratégica de la ciberseguridad, no de insuficiencia técnica. Esta es la contribución diagnóstica más original del análisis de literatura. (Cheng & Wang, 2022)

identificaron la desalineación entre estrategia TI y estrategia de seguridad como el predictor más consistente de brechas de madurez en IES, convergiendo con los hallazgos identificados en el contexto colombiano.

La progresión en esta dimensión sigue la lógica de la Teoría de Capacidades (Teece et al., 1997): los Niveles 1 y 2 corresponden a organizaciones sin capacidad de sensing estratégico; el Nivel 3 introduce las estructuras formales que habilitan la gobernanza activa; el Nivel 4 integra la ciberseguridad en la planeación institucional (seizing); y el Nivel 5 incorpora la gobernanza de IA y la vigilancia regulatoria como capacidades de transforming.

3.2. Indicadores Detallados por Nivel

Nivel 1 - Reactivo: Sin gobernanza formal

La ciberseguridad no existe como función institucional reconocida. Sin política, sin responsable con mandato formal, sin presupuesto propio. Las decisiones de seguridad son enteramente ad hoc, respondiendo a incidentes ya ocurridos. El 90,4% de los expertos calificó el nivel de madurez de las IES colombianas como medio o bajo, lo que indica que la mayoría se sitúa entre los Niveles 1 y 2.

- **I1.G.1:** No existe política institucional de ciberseguridad aprobada por la máxima autoridad institucional. No hay documento formal con fecha, firma, alcance definido y mecanismo de actualización. Verificación: revisión documental del repositorio de políticas institucionales.
- **I1.G.2**: No existe rol formal de responsable de seguridad con mandato institucional reconocido. Ningún cargo tiene funciones de ciberseguridad en su descripción formal. Verificación: revisión del organigrama y de las descripciones de cargo vigentes del área de TI.
- **I1.G.3:** No existe línea presupuestal propia para ciberseguridad; el gasto es contingente a incidentes ocurridos. La inversión en seguridad no aparece como rubro diferenciado en el presupuesto de TI. Verificación: revisión del presupuesto de TI y del plan de compras institucional.

Nivel 2 - Emergente: Política básica sin seguimiento

Existe una política aprobada desde lo formal, pero sin revisión periódica ni mecanismos de seguimiento. El responsable de TI asume seguridad sin mandato directivo formal. La asignación presupuestal existe, pero diluida en el presupuesto general de TI.

- **I2.G.1:** Política de ciberseguridad aprobada formalmente, pero no revisada en los últimos 24 meses. El contenido no ha sido actualizado ante cambios del entorno de amenazas. Verificación: revisión de la fecha de última actualización y comparación con eventos normativos relevantes desde esa fecha.
- **I2.G.2:** Responsable TI asume funciones de seguridad sin mandato formal ni acceso al nivel directivo. El rol no está formalizado en una descripción de cargo ni tiene mecanismos de reporte directo a la dirección. Verificación: revisión de la descripción de cargo del responsable de TI.
- **I2.G.3:** Asignación presupuestal básica para ciberseguridad incluida dentro del presupuesto general de TI, sin plan plurianual de inversión. Verificación: revisión del presupuesto de TI con identificación de partidas vinculadas a seguridad.

Nivel 3 - Estructurado: CISO formal y comité activo

Rol de CISO formalizado con descripción de cargo, KPIs y acceso al comité directivo con periodicidad mínima trimestral. Política revisada anualmente alineada con un marco normativo reconocido. Línea presupuestal propia con plan de inversión documentado. La UNAD se posiciona en este nivel: 78,6% apoyo directivo, 64,3% políticas formales actualizadas, línea presupuestal identificable.

- **I3.G.1:** Existe rol formal de CISO o equivalente con descripción de cargo, KPIs y acceso al comité directivo con frecuencia mínima trimestral. El cargo tiene mandato institucional que le permite imponer controles sobre todas las áreas que manejan activos de información. Verificación: revisión de la descripción de cargo, organigrama y actas del comité directivo que acrediten la participación del CISO.
- **I3.G.2:** La política de ciberseguridad se revisa y actualiza anualmente y está formalmente alineada con la ISO 27001:2022 o el NIST CSF 2.0. La alineación

garantiza que la política cubre los dominios normativos mínimos requeridos. Verificación: revisión del documento de política con su fecha de actualización y del mapeo con el marco normativo declarado.

- **I3.G.3:** La ciberseguridad tiene línea presupuestal independiente del presupuesto general de TI, con plan de inversión anual documentado y aprobado por la autoridad competente. Verificación: revisión del presupuesto institucional con identificación del rubro de ciberseguridad y del plan de inversión anual.

Nivel 4 - Gestionado: Integración estratégica plena

La ciberseguridad aparece en el Plan de Desarrollo Institucional con metas medibles, indicadores cuantitativos y responsables formalizados. Tablero de control revisado mensualmente por el comité directivo. Reportes al Consejo Superior semestral. La distinción crítica con el Nivel 3: la integración estratégica y la medición cuantitativa, no la existencia de estructuras de gobernanza (que ya existen en N3).

- **I4.G.1**: La ciberseguridad está incluida en el Plan de Desarrollo Institucional con metas específicas, indicadores de cumplimiento y responsables formalizados. Verificación: revisión del PDI vigente con identificación del componente de ciberseguridad.
- **I4.G.2:** Existe tablero de control de ciberseguridad con KPIs definidos, revisado mensualmente por el comité directivo con evidencia documentada de los resultados y las decisiones tomadas. Verificación: revisión de las actas del comité directivo y del tablero de control.
- **I4.G.3:** Los riesgos de ciberseguridad son reportados formalmente al Consejo Superior o Académico con periodicidad semestral mínima, con evidencia documental de los reportes. Verificación: revisión de las actas del Consejo Superior que incluyan reportes de ciberseguridad.

Nivel 5 - Resiliente: Gobernanza adaptativa de IA

Gobernanza de IA integrada con la política de ciberseguridad alineada con el NIST AI RMF v1.0 (Tabassi, 2023) e ISO 42001:2023. Mecanismos de vigilancia tecnológica que anticipan cambios regulatorios (EU AI Act, criptografía post cuántica) con plan de adaptación

institucional. Capacidad de transforming organizacional plena según la Teoría de Capacidades Dinámicas.

- **I5.G.1**: Existe política de gobernanza de IA integrada con la política de ciberseguridad, alineada con el NIST AI RMF v1.0 (Tabassi, 2023) e ISO 42001:2023. Cubre los cuatro componentes del AI RMF (Govern, Map, Measure, Manage) y los controles del Anexo A relevantes para el contexto universitario. Verificación: revisión del documento de política de gobernanza de IA y su mapeo con los marcos referenciados.
- **I5.G.2:** Existen mecanismos formales de vigilancia tecnológica que anticipan cambios regulatorios (European Commision, 2024), (National Institute of Standards and Technology (US), 2024) con evaluación de impacto documentada y plan de adaptación institucional aprobado. Verificación: revisión del informe de vigilancia tecnológica y del plan de adaptación regulatoria.

3.3. Indicadores - Dimensión Gobernanza

Ilustración 3.
Indicadores relacionados con la dimensión de la Gobernanza

Nota. Tabla 3. Indicadores de la Dimensión Gobernanza (D1-GOB). 8 indicadores totales (I1.G.1 a I5.G.2). Los indicadores son criterios observables y verificables mediante revisión documental, entrevista semiestructurada o inspección técnica. Elaboración propia.

4. DIMENSIÓN 2: TALENTO HUMANO Y COMPETENCIAS K-S-A

Código: D2-TAL · **Indicadores:** 13 (I1.T.1 a I5.T.3) ·

Respaldo: 98,1% de expertos señala déficit · Cuádruple convergencia especialista IA (84,6% - 92,9%)

Referentes: (NIST, 2020) · (ENISA, 2022) · (REDSIIUNAD, 2025) · (Murphy et al., 2023) · (ISC2, 2024)

4.1. Fundamento y Justificación

El talento humano es la dimensión con la brecha más contundente: el 98,1% de los expertos señala insuficiencia de talento especializado y el 63,2% evalúa la formación actual como limitada o deficiente. Esta dimensión integra la triada: **Conocimientos - Habilidades - Capacidades** (K-S-A: Knowledge, Skills, Abilities) del NICE (Petersen et al., 2020), el European Cybersecurity Skills Framework de (ENISA, 2022) y los perfiles reales de la (REDSIIUNAD, 2025), el primer documento que formaliza la estructura de equipos de ciberseguridad de la UNAD.

El hallazgo de mayor robustez estadística es la cuádruple convergencia sobre el perfil de especialista en IA y ciberseguridad como el más demandado para el horizonte 2026 - 2029: el 84,6% de los expertos (I1), el 87,5% de los actores gubernamentales (I5), el 84,6% de los docentes (I3) y el 92,9% de los estudiantes (I4) lo identificaron como el perfil prioritario. Ningún otro perfil alcanzó esta convergencia en cuatro grupos simultáneamente. Este hallazgo determina el indicador **I5.T.1.**

El indicador más original del modelo completo es **I3.T.1**: la existencia de dos equipos diferenciados: analítico-estratégico y operativo, como criterio de madurez del Nivel 3. Ningún modelo de referencia existente especifica esta arquitectura de equipos para IES. Es una contribución derivada directamente de la (REDSIIUNAD, 2025): Equipo Analítico - Estratégico (Líder CSIRT, Arquitecto de Ciberseguridad e Innovación, Analista en Inteligencia de Ciberamenazas, Monitor de Análisis de Seguridad, Analista de Seguridad en Infraestructura y Endurecimiento, Gestor de Cualificación en Ciberseguridad) y Equipo Operativo (Coordinador de Respuesta a Incidentes - Project Manager, Gestor de Seguridad de Aplicaciones y Acceso, Gestor de Seguridad de Bases de Datos, Gestor de Seguridad en Servidores). Igualmente, original es **I3.T.3**: la articulación formal entre el equipo de ciberseguridad y los programas académicos, una ventaja estructural exclusiva de las IES que el modelo captura como criterio de madurez.

4.2. Indicadores Detallados por Nivel

Nivel 1 - Reactivo: Sin roles definidos

Sin roles formales de ciberseguridad en ningún cargo. El personal de TI asume funciones de seguridad sin formación específica, sin mandato y sin descripción de cargo que las respalde. Sin plan de competencias ni criterios de contratación por perfil.

- **I1.T.1:** No existe descripción de cargo con funciones específicas de ciberseguridad en ningún rol institucional. Verificación: revisión de descripciones de cargo del área de TI y de cualquier área que maneje activos críticos.
- **I1.T.2:** El personal de TI no ha recibido formación formal en ciberseguridad en los últimos 24 meses. Verificación: revisión de los registros de capacitación del área de TI.
- **I1.T.3:** No existe plan de desarrollo de competencias en ciberseguridad ni criterios de contratación basados en perfil de seguridad. Verificación: revisión del plan de formación del área de TI y de las convocatorias de contratación recientes.

Nivel 2 - Emergente: Roles básicos informales

Roles básicos asignados informalmente. Al menos un integrante con certificación básica. Capacitación esporádica sin plan estructurado ni evaluación de impacto.

- **I2.T.1:** Al menos un integrante del equipo de TI cuenta con certificación básica en ciberseguridad (CompTIA Security+, CCNA Security o equivalente reconocido). Verificación: revisión de los certificados del personal de TI o ciberseguridad.
- **I2.T.2:** Se realizan actividades de capacitación en ciberseguridad al menos una vez por año, aunque sin plan estructurado ni evaluación de impacto sobre las competencias. Verificación: revisión del registro de capacitaciones del último año.
- **I2.T.3:** Las funciones básicas de seguridad requeridas han sido identificadas, aunque sin mapeo formal a perfiles de cargo. Verificación: entrevista con el responsable de TI.

Nivel 3 - Estructurado: Equipo o Equipos con perfiles NICE

Equipos diferenciados con perfiles formalizados. K-S-A documentadas por rol. Articulación formal con programas académicos. Indicador diferenciador: **I3.T.1 -** estructura dual analítico - estratégico y operativo.

- **I3.T.1:** Existe uno o varios equipos diferenciados, con perfiles de cargo formalizados y funciones delimitadas. Indicador diferenciador del modelo: ningún marco previo especifica esta arquitectura para IES. Verificación: organigrama del área de ciberseguridad y descripciones de cargo de los roles de cada equipo.
- **I3.T.2:** Los perfiles de cargo están alineados con al menos un marco internacional (NICE/NIST SP 800-181r1 o ECSF/ENISA), con las K-S-A documentadas por rol. Verificación: descripciones de cargo y mapeo con el marco internacional declarado.
- **I3.T.3:** Existe articulación formal entre el equipo de ciberseguridad y los programas académicos para transferencia de conocimiento y práctica. En la UNAD: vínculo ECBTI - CSIRT Académico UNAD. Verificación: documento que formaliza la articulación y actividades realizadas en el último año.

Nivel 4 - Gestionado: Formación continua medida

Plan de certificación anual por perfil con presupuesto y seguimiento. Evaluación de brechas K-S-A por rol. El Gestor de Cualificación en Ciberseguridad, perfil formalizado, mide la madurez en prácticas seguras de toda la comunidad universitaria.

- **I4.T.1:** Existe plan de formación y certificación anual por perfil de cargo, con presupuesto asignado y seguimiento de cumplimiento documentado. Verificación: plan de formación anual y porcentaje de cumplimiento.
- **I4.T.2:** Se aplica instrumento de evaluación de brechas K-S-A al menos una vez por año para cada rol del equipo de ciberseguridad, con plan de cierre documentado. Verificación: instrumento de evaluación de competencias y planes de cierre de brechas.
- **I4.T.3:** El Gestor de Cualificación en Ciberseguridad (o equivalente) mide el nivel de madurez en prácticas seguras de toda la comunidad universitaria (docentes, estudiantes, personal administrativo) con métricas documentadas y plan de mejora. Verificación: informe más reciente de medición de madurez en cultura de seguridad de la comunidad institucional.

Nivel 5 - Resiliente: Especialistas en IA y redes CSIRT internacionales

Perfil formal de especialista en IA y ciberseguridad. Participación en redes CSIRT internacionales. Ejercicios de Red Team sistemáticos o TTX anuales con informe de hallazgos. Capacidad de transforming del equipo: aprender de amenazas emergentes, de otras instituciones y de sus ejercicios ofensivos para reconfigurar la defensa.

- **I5.T.1:** El equipo cuenta con perfil formal de especialista en IA y ciberseguridad, con competencias documentadas en amenazas potenciadas por ML (adversarial attacks, prompt injection, deepfake engineering) y gobernanza ética de IA según el NIST AI RMF. Indicador derivado de la cuádruple convergencia identificada (84,6% - 92,9%). Verificación: perfil de cargo y certificaciones del especialista.
- **I5.T.2:** La institución participa activamente en al menos una red nacional o internacional de CSIRT o equipos de respuesta universitario, con aporte de threat intelligence documentado y participación en ejercicios conjuntos. Verificación: acuerdos de membresía y registros de participación.

- **I5.T.3:** El equipo ejecuta ejercicios de Red Team o simulaciones de ataque al menos una vez por año, con informe formal de hallazgos, plan de remediación y seguimiento de cierre verificable. Verificación: informe del último ejercicio y plan de remediación.

4.3. Indicadores: Dimensión Talento Humano

Ilustración 4.
Indicadores: Dimensión Talento Humano

*Nota. Ilustración 4. Indicadores de la Dimensión Talento Humano (D2-TAL). 13 indicadores totales. El indicador **I3.T.1** es la contribución más original del modelo completo: ningún marco de referencia previo especifica la estructura dual analítico-estratégico/operativo para IES. Fundamento operativo: REDSIIUNAD (2025). Elaboración propia.*

5. DIMENSIÓN 3: GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

Código: D3-RIE · **Indicadores:** 15 (I1.R.1 a I5.R.3) · **Respaldo:** 65,4% mayor respaldo cuantitativo en Instrumento 1 del OE2

Referentes: ISO 27001:2022 Cláusula 6 · (National Institute of Standards and Technology, 2024b) Función Identify ·MSPI (MinTIC, 2025) · (REDSIIUNAD, 2025) Tabla de Validaciones

5.1. Fundamento y Justificación

La gestión de riesgos es la dimensión con el mayor respaldo cuantitativo en el Instrumento 1 (65,4% de los expertos la identifica como dimensión prioritaria), situándose por encima de la gobernanza (63,5%) y la seguridad de IA (61,5%). La progresión sigue el ciclo Plan-Do-Check-Act de la ISO 27001:2022 y la función Identify del (National Institute of Standards and Technology, 2024b), que comprende la gestión de activos (ID.AM), la evaluación de riesgos (ID.RA) y la mejora continua (ID.IM). El MSPI del MinTIC colombiano provee el referente de política pública nacional más relevante.

El indicador más original de esta dimensión: **I4.R.3,** contiene los tiempos de validación de seguridad para puesta en producción de servicios tecnológicos (REDSIIUNAD, 2025). Ningún modelo de madurez para IES previo incluye tiempos operativos específicos como criterios de nivel. Su origen en evidencia empírica directa del caso piloto le otorga validez contextual que los indicadores derivados de marcos internacionales no tienen.

La síntesis de la progresión en esta dimensión: Nivel 1, no sabe qué tiene ni qué riesgos enfrenta; Nivel 2, comienza a identificar activos sin metodología; Nivel 3, formaliza la metodología con ciclo anual; Nivel 4, integra el análisis de riesgos en las decisiones de

inversión con tiempos operativos definidos; Nivel 5, anticipa riesgos emergentes mediante threat intelligence continua.

5.2. Indicadores Detallados por Nivel

Nivel 1 - Reactivo: Sin inventario de activos

Sin ningún registro de activos de información crítica. Sin evaluaciones de riesgo. Sin plan de tratamiento. El único mecanismo de respuesta es la reacción a incidentes ya materializados.

- **I1.R.1:** No existe inventario documentado y clasificado de activos de información crítica. Sin inventario es imposible saber qué proteger ni cómo priorizar controles. Verificación: consulta al área de TI sobre la existencia de un registro formal de activos de información.
- **I1.R.2:** No se realizan evaluaciones de riesgo formales. Las vulnerabilidades se atienden únicamente cuando se materializan como incidentes con daño real. Verificación: revisión de la documentación del área de TI; ausencia de metodología de evaluación de riesgos aplicada.
- **I1.R.3:** No existe plan de tratamiento de riesgos ni registro de riesgos aceptados institucionalmente. Verificación: consulta al área de TI y revisión documental.

Nivel 2 - Emergente: Inventario básico y análisis ad hoc

Inventario básico sin clasificación formal por criticidad ni propietario. Evaluaciones de vulnerabilidades al menos anuales sin metodología estandarizada. Registro básico de incidentes sin análisis sistemático.

- **I2.R.1:** Existe inventario de activos de información documentado, aunque sin clasificación formal por nivel de criticidad ni propietario asignado por sistema. Verificación: revisión del inventario existente.
- **I2.R.2:** Se realizan evaluaciones de vulnerabilidades al menos una vez por año, aunque sin metodología estandarizada ni seguimiento formal de los hallazgos. Verificación: revisión de los informes de evaluación del último año.

- **I2.R.3:** Existe registro básico de incidentes de seguridad, aunque sin análisis sistemático de causas raíz ni sistematización de lecciones aprendidas. Verificación: revisión del registro de incidentes.

Nivel 3 - Estructurado: Metodología formal periódica

Metodología formal con ciclo anual aprobado. Inventario clasificado por criticidad con propietarios. Plan de tratamiento con seguimiento trimestral. La UNAD está en transición hacia este nivel: tiene tiempos de validación formalizados en la REDSIIUNAD (2025) pero consolida el ciclo completo de evaluación de riesgos.

- **I3.R.1:** El inventario de activos está clasificado por criticidad (alta/media/baja) con propietario formal asignado para cada sistema crítico y revisión semestral documentada. Verificación: revisión del inventario con su clasificación y propietarios asignados.
- **I3.R.2:** Se aplica metodología formal de evaluación de riesgos (Magerit, OCTAVE, ISO 31000 o equivalente reconocido) con ciclo anual aprobado institucionalmente y documentado. Verificación: informe de evaluación de riesgos más reciente y metodología aplicada.
- **I3.R.3:** Existe plan de tratamiento de riesgos con acciones documentadas, responsables asignados, plazos definidos y seguimiento trimestral documentado por el CSIRT o el Oficial de Seguridad. Verificación: plan de tratamiento e informes de seguimiento trimestral.

Nivel 4 - Gestionado: Riesgos en las decisiones de inversión TI

El análisis de riesgos es condición formal para proyectos tecnológicos y adquisiciones. Gestión de riesgo en terceros con cláusulas contractuales.

- **I4.R.1:** El análisis de riesgos de ciberseguridad es condición formal para la aprobación de proyectos tecnológicos y adquisición de sistemas de terceros. Ningún proyecto entra a implementación sin evaluación de riesgos previa aprobada. Verificación: proceso de aprobación de proyectos TI e informes de evaluación de proyectos recientes.

- **I4.R.2:** Existe proceso formal de gestión de riesgo en terceros y proveedores con cláusulas de seguridad contractuales verificadas antes de la puesta en producción. Verificación: contratos de servicios TI con cláusulas de seguridad y proceso de verificación.
- **I4.R.3:** Los tiempos de validación de seguridad para puesta en producción están definidos y se cumplen sistemáticamente: 7 días hábiles para servidores, 10 días hábiles para aplicaciones y 3 días hábiles para asignación de usuarios e integraciones de sistemas (REDSIIUNAD, 2025). Primer indicador cuantitativo operativo del modelo. Verificación: proceso formal de puesta en producción y registros de tiempos de validación.

Nivel 5 - Resiliente: Gestión predictiva con threat intelligence

Threat intelligence trimestral integrado al ciclo de evaluación de riesgos. Modelos de amenazas actualizados ante IA generativa y criptografía post cuántica. Hallazgos de Red Team integrados al registro de riesgos con plan de remediación verificable.

- **I5.R.1:** El Analista de Inteligencia de Ciberamenazas, perfil formalizado en la REDSIIUNAD (2025), produce informes de threat intelligence al menos trimestrales, integrados formalmente al ciclo de evaluación de riesgos con evidencia de actualizaciones al registro de riesgos. Verificación: informes de threat intelligence e integración en el registro de riesgos.
- **I5.R.2:** Los modelos de amenazas institucionales se actualizan tras cada incidente significativo y ante cambios relevantes del entorno tecnológico, incluyendo nuevas amenazas potenciadas por IA generativa y estándares emergentes de criptografía post cuántica. Verificación: modelo de amenazas vigente e historial de actualizaciones.
- **I5.R.3:** Los hallazgos de los ejercicios de evaluación ofensiva (Red Team, pentesting) se integran formalmente al registro de riesgos con plan de remediación documentado, plazos definidos y seguimiento verificable. Verificación: informe del último ejercicio ofensivo e integración al registro de riesgos.

5.3. Indicadores - Dimensión Gestión de Riesgos

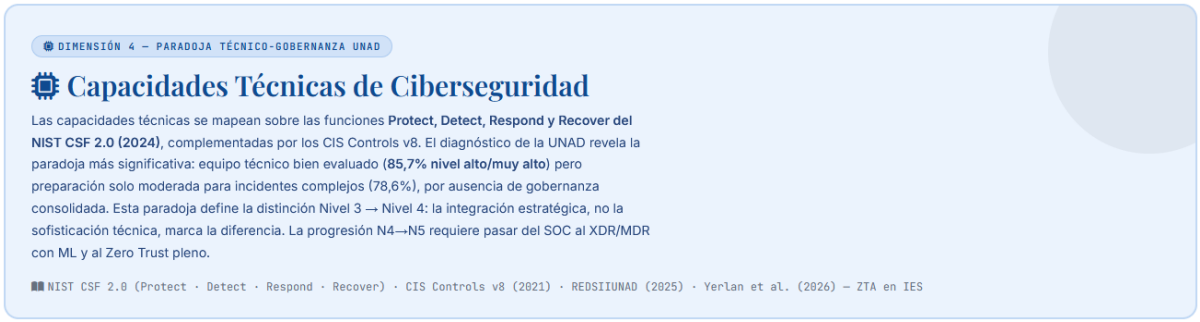
Ilustración 5.
Indicadores - Dimensión Gestión de Riesgos

Nota. Ilustración 5. Indicadores de la Dimensión Gestión de Riesgos (D3-RIE). 15 indicadores totales. El indicador I4.R.3 es el primer indicador cuantitativo operativo del modelo, con tiempos derivados directamente de la REDSIIUNAD (2025). Elaboración propia.

6. DIMENSIÓN 4: CAPACIDADES TÉCNICAS DE CIBERSEGURIDAD

Código: D4-TEC · **Indicadores:** 15 (I1.C.1 a I5.C.3) · **Respaldo:** Diagnóstico UNAD: SIEM 50%, continuidad 50%, equipo técnico alto/muy alto 85,7%

Referentes: (National Institute of Standards and Technology, 2024b) Protect·Detect·Respond·Recover · CIS Controls v8 (CIS, 2021) · (REDSIIUNAD, 2025) · (Harun Or Rashid & Mustafa, 2026)



6.1. Fundamento y Justificación

La recopilación de información revela la paradoja más significativa de la investigación: el 85,7% del personal evalúa favorablemente el nivel técnico del equipo (alto o muy alto), pero el 78,6% reconoce solo preparación moderada para incidentes complejos. Esta paradoja es capturada exactamente por la distinción entre el Nivel 3 y el Nivel 4: una institución puede tener SIEM operativo, MFA implementado y plan de respuesta probado (N3) pero carecer del SOC 24/7, el BCP - DRP formalmente probado y el hardening sistemático que caracterizan el N4. La distinción no es de sofisticación técnica sino de integración operacional y estratégica.

La progresión está mapeada sobre las cuatro funciones operativas del (National Institute of Standards and Technology, 2024b): Protect (controles preventivos), Detect (monitoreo y detección de anomalías), Respond (respuesta coordinada) y Recover (restauración y aprendizaje post-incidente), complementadas con los CIS Controls v8 (CIS, 2021) para la priorización operativa. Los perfiles del Equipo Operativo de la (REDSIIUNAD, 2025) proveen el referente operativo para los indicadores de los Niveles 3 y 4. La transición más exigente es N4 a N5: requiere pasar del SOC centralizado al XDR - MDR con ML, la implementación plena de Zero Trust y el threat hunting proactivo. (Harun Or Rashid & Mustafa, 2026)

documentaron que la preparación de gobernanza para ZTA en IES está más rezagada que la preparación técnica.

6.2. Indicadores Detallados por Nivel

Nivel 1 - Reactivo: Controles básicos aislados

Sin plan de respuesta a incidentes - IR, sin controles de acceso formalizados, sin gestión de parches. Los privilegios de administrador no están diferenciados, lo que expone a la institución a riesgos de insider threat y escalada de privilegios.

- **I1.C.1:** No existe plan de respuesta a incidentes documentado ni equipo designado para gestionarlos. Verificación: consulta al área de TI y revisión documental.
- **I1.C.2:** No existen controles de acceso formalizados; los privilegios de administrador no están diferenciados por rol ni función. Verificación: revisión de la gestión de cuentas privilegiadas en los sistemas críticos.
- **I1.C.3:** No existe proceso formal de gestión de parches ni actualización periódica de sistemas operativos y aplicaciones críticas. Verificación: revisión del estado de actualización de los sistemas críticos.

Nivel 2 - Emergente: Controles básicos implementados

Controles básicos de protección perimetral. Control de acceso con mínimo privilegio. Plan IR documentado pero no probado formalmente.

- **I2.C.1:** Existe firewall perimetral, antivirus - antimalware y copias de seguridad con periodicidad definida y verificación básica de restauración al menos trimestral. Verificación: registros de backups y pruebas de restauración.
- **I2.C.2:** Existe control de acceso básico con diferenciación de usuarios administradores siguiendo el principio de mínimo privilegio. Verificación: configuración de cuentas en sistemas críticos y política de accesos.
- **I2.C.3:** Existe plan básico de respuesta a incidentes documentado con rutas de escalamiento y roles mínimos, aunque no probado formalmente mediante simulacro o tabletop exercise TTX. Verificación: revisión del plan y su historial de actualizaciones.

Nivel 3 - Estructurado: SIEM, MFA e IR probado

SIEM operativo con correlación de eventos y alertas configuradas. MFA en todos los sistemas críticos. Plan IR probado mediante simulacro. El diagnóstico de la UNAD la ubica en este nivel: SIEM en el 50% de los casos, continuidad operativa como fortaleza en el 50%.

- **I3.C.1:** Sistema SIEM operativo con correlación de eventos de múltiples fuentes, dashboards activos y alertas configuradas para los sistemas críticos institucionales. Verificación: acceso al panel del SIEM con demostración de alertas activas y registros de correlación.
- **I3.C.2:** Autenticación multifactor (MFA) implementada en todos los sistemas críticos y en todos los accesos privilegiados de administrador. Verificación: prueba técnica de acceso con verificación del MFA activo.
- **I3.C.3:** El plan de respuesta a incidentes ha sido probado mediante al menos un simulacro o tabletop exercise en los últimos 12 meses, con informe de resultados y actualización del plan. Verificación: informe del último simulacro y actualizaciones derivadas.

Nivel 4 - Gestionado: SOC 24/7, BCP/DRP probado y hardening sistemático

SOC con monitoreo continuo 24/7 con métricas MTTD y MTTR. BCP y DRP probados con RTO/RPO definidos. Hardening sistemático conforme a CIS Benchmarks verificado semestralmente. La prueba formal del BCP/DRP distingue instituciones que han verificado que sus planes funcionan de las que solo los tienen documentados.

- **I4.C.1:** Existe SOC propio o contratado (MSSP) con monitoreo 24/7, escalamiento documentado y métricas de tiempo medio de detección (MTTD) y tiempo medio de respuesta (MTTR) registradas. Verificación: documentación del SOC con métricas de los últimos tres meses.
- **I4.C.2:** Existen Plan de Continuidad del Negocio (BCP) y Plan de Recuperación ante Desastres (DRP) documentados, probados al menos una vez por año con RTO y RPO

definidos y verificados para los sistemas críticos. Verificación: plan y el informe de la última prueba de recuperación con tiempos documentados.

- **I4.C.3:** Se implementa estrategia de hardening en servidores, bases de datos y endpoints conforme a los CIS Benchmarks, con verificación semestral documentada. Verificación: informes de verificación de hardening más recientes y Benchmarks aplicados.

Nivel 5 - Resiliente: XDR, Zero Trust pleno y threat hunting proactivo

XDR/MDR con análisis de comportamiento basado en Machine Learnign - ML. Zero Trust en toda la infraestructura crítica. Threat hunting proactivo trimestral con hipótesis basadas en threat intelligence. La detección por comportamiento descubre amenazas que no generan firmas conocidas, incluyendo las potenciadas por IA generativa.

- I5.C.1: La plataforma de detección incorpora capacidades XDR o MDR con análisis de comportamiento basado en ML, con alertas integradas al ciclo del CSIRT y registros de amenazas detectadas por comportamiento anómalo. Verificación: registros de detección del XDR/MDR con casos de amenazas detectadas por comportamiento.
- I5.C.2: La arquitectura Zero Trust está implementada en toda la infraestructura crítica, con verificación continua de identidad, dispositivo y contexto en cada solicitud de acceso, independientemente de la ubicación del usuario. Verificación: arquitectura de red con demostración del modelo de verificación continua.
- I5.C.3: El equipo ejecuta ejercicios de threat hunting proactivo al menos trimestralmente, con hipótesis documentadas basadas en threat intelligence, proceso de búsqueda documentado e informe de hallazgos independiente de las alertas del SIEM. Verificación: informes de threat hunting de los últimos cuatro ciclos trimestrales.

6.3. Indicadores - Dimensión Capacidades Técnicas

Ilustración 6.
Indicadores - Dimensión Capacidades Técnicas

Nota. Ilustración 6. Indicadores de la Dimensión Capacidades Técnicas (D4-TEC). 15 indicadores totales. La paradoja técnico-gobernanza de la UNAD (equipo técnico 85,7% alto/muy alto vs preparación moderada para incidentes 78,6%) fundamenta la distinción entre los Niveles 3 y 4 en esta dimensión. Elaboración propia.

7. DIMENSIÓN 5: SEGURIDAD DE INTELIGENCIA ARTIFICIAL (ISO 42001:2023)

Código: D5-IA ★ · **Indicadores:** 20 (I1.IA.1 a I5.IA.5) — DIMENSIÓN DIFERENCIADORA DEL MODELO

Referentes: NIST AI RMF v1.0 (Tabassi, 2023) · ISO/IEC 42001:2023 (ISO, 2023) Cláusulas 6 - 10 + Anexo A · (European Commision, 2024) · NIST FIPS 203/204/205

Respaldo empírico: 100% unanimidad en dos instrumentos simultáneamente · 82,7% expertos señala ausencia de políticas IA · 93% personal TI UNAD confirma ausencia de lineamientos

7.1. Fundamento y Justificación: La Dimensión Diferenciadora

La Seguridad de IA es la dimensión que diferencia el MMCC-IES de todos los modelos de referencia existentes. Ningún modelo disponible, CMM/GCSCC (2021), NIST CSF 2.0 (2024), los modelos sectoriales de (Salam et al., 2026) y (Almomani et al., 2021), la incorpora como dimensión autónoma con indicadores específicos por nivel de madurez. Su inclusión está respaldada por la evidencia empírica más contundente: el único ítem que alcanzó unanimidad absoluta (100%) es el que identifica la IA como área curricular más urgente de fortalecer (Instrumento 3), y el único resultado con unanimidad en el diagnóstico piloto UNAD es la evaluación negativa de la preparación ante amenazas de IA (Instrumento 2).

La ISO/IEC 42001:2023 es el primer estándar internacional de Sistemas de Gestión de Inteligencia Artificial (SGIA). Publicado en diciembre de 2023, su Anexo A contiene 38 controles en nueve dominios que el modelo MMCC-IES operacionaliza en cuatro ejes integrados con los niveles de madurez:

- **Eje 1:** Transparencia y Explicabilidad Algorítmica (XAI): Los algoritmos que apoyan decisiones de calificación, admisión o evaluación docente deben ser documentados y explicables. Referentes: Anexo A.7 (Documentación del sistema IA) y A.8.4 (Transparencia e interpretabilidad). Presente desde el Nivel 2 con descripción básica; completo en el Nivel 4 con XAI verificable.
- **Eje 2:** Control de Sesgos: Los sistemas de IA de alto riesgo deben evaluarse por equidad y sesgo en grupos protegidos (género, etnia, condición socioeconómica). Referentes: Anexo A.6.2 (Calidad de datos) y A.8.5 (Equidad). Incorporado en el Nivel 3 con el indicador **I3.IA.2.** Crítico para IES colombianas donde los sistemas de calificación automatizada pueden reproducir desigualdades estructurales.
- **Eje 3:** Gobernanza del Ecosistema de IA (Terceros y Cadena de Suministro): Las IES que usan LMS externos, APIs de IA generativa de terceros y modelos preentrenados cuyos datos de entrenamiento no controlan deben gestionar el riesgo de su ecosistema IA completo. Referentes: Anexo A.9 (Proveedores de IA) y A.9.2 (Cadena de suministro IA). Desde el Nivel 3 con contratos y completo en el Nivel 5.
- **Eje 4:** Auditoría Integral del SGIA y Mejora Continua: El SGIA debe auditarse internamente al menos una vez al año (ISO 42001 Cláusula 9.2), revisarse por la dirección y someterse a ciclos de mejora continua (Cláusula 10). El Nivel 5 incorpora el proceso formal de certificación con Statement of Applicability documentado.

7.2. Indicadores Detallados por Nivel

Nivel 1 - Reactivo: Sin política de IA - Opacidad total

El Nivel 1 corresponde a: el 93% del personal TI no puede confirmar la existencia de lineamientos para el uso seguro de IA. Sin SGIA, sin política, con Shadow AI completamente libre. Los algoritmos que toman decisiones institucionales no están documentados ni son explicables. Opacidad total. Esta es la brecha más urgente: documentada por unanimidad en cuatro grupos de los cinco instrumentos.

- **I1.IA.1:** No existe política de uso aceptable de IA ni definición del alcance de un SGIA (ISO 42001:2023 Cláusula 4.3). No hay documento institucional que defina qué

herramientas de IA están autorizadas, para qué usos y con qué restricciones sobre los datos procesables. Verificación: consulta al área de TI y de gestión institucional sobre la existencia de políticas de IA.

- **I1.IA.2:** No existe inventario de sistemas de IA en uso institucional; el Shadow AI, uso de herramientas de IA generativa externas sin autorización es completamente libre y sin controles. Verificación: entrevista con el área de TI sobre el mapeo de herramientas IA en uso.
- **I1.IA.3:** Los algoritmos que apoyan o toman decisiones institucionales de alto impacto (calificación, detección de plagio, verificación de identidad) no están documentados ni son explicables para los afectados. Opacidad algorítmica total. Verificación: identificación de sistemas IA de decisión en uso y consulta sobre su documentación.

Nivel 2 - Emergente: Política básica e inventario inicial

Primer paso del SGIA: política básica aprobada con lista de herramientas autorizadas y criterios de datos. Primer ejercicio de identificación de Shadow AI. Los sistemas de IA de alto impacto tienen descripción básica del algoritmo y sus limitaciones, primer paso de transparencia según el Anexo A.8.2.

- **I2.IA.1:** Existe política básica de uso aceptable de IA aprobada institucionalmente, con lista de herramientas autorizadas y criterios básicos de clasificación de datos procesables en sistemas externos de IA (ISO 42001:2023 Cláusula 5.2 + Anexo A.2). La política debe existir, tener firma de autoridad competente y definir explícitamente qué herramientas están autorizadas para qué usos. Verificación: revisión del documento de política y lista de herramientas autorizadas.
- **I2.IA.2:** Se ha realizado al menos un ejercicio de identificación de Shadow AI con registro de hallazgos documentado y plan de gestión. Verificación: informe del ejercicio de identificación de Shadow AI.
- **I2.IA.3:** Los sistemas de IA de alto impacto utilizados (calificación, detección de plagio, verificación de identidad) tienen descripción básica del algoritmo, sus datos de entrada, sus limitaciones conocidas y los contactos responsables — Transparencia

inicial (Anexo A.8.2). Verificación: revisión de la documentación básica de los sistemas IA de alto impacto.

Nivel 3 - Estructurado: SGIA activo con los cuatro ejes operativos

El Nivel 3 es el más exigente de la Dimensión 5: incorpora cuatro indicadores que activan los tres primeros ejes de la ISO 42001:2023. El AI Impact Assessment (AIIA) es la herramienta central de evaluación previa a la adopción. La evaluación de sesgos por grupos protegidos es la primera medición de equidad algorítmica. Las cláusulas contractuales con proveedores IA son la primera manifestación del control del ecosistema. El human-in-the-loop[1] garantiza que ninguna decisión de alto impacto sobre personas sea enteramente automatizada.

- **I3.IA.1:** Todo sistema de IA nuevo requiere la realización y aprobación de un AI Impact Assessment (AIIA)[2] documentado antes de su adopción institucional. Evalúa el impacto ético, social, legal y de ciberseguridad (ISO 42001:2023 Cláusula 6.1.2 + Anexo A.5). Verificación: proceso de aprobación de nuevos sistemas IA y AIIA de adopciones recientes.
- **I3.IA.2:** Los sistemas de IA de alto riesgo tienen evaluación de sesgos documentada con métricas de equidad por grupos protegidos: género, etnia, condición socioeconómica (Anexo A.6.2 + A.8.5). Eje 2, Control de sesgos. Verificación: informe de evaluación de sesgos del último sistema IA de alto riesgo adoptado.
- **I3.IA.3:** Los contratos con proveedores de sistemas IA incluyen cláusulas de transparencia sobre el funcionamiento del sistema, reporte de incidentes vinculados a IA y derecho de auditoría técnica por parte de la institución (Anexo A.9). Eje 3, Gobernanza del ecosistema. Verificación: contratos de sistemas IA con verificación de las cláusulas requeridas.
- **I3.IA.4:** Existe mecanismo formal de supervisión humana (human-in-the-loop) para las decisiones automatizadas de alto impacto sobre estudiantes o personal. Ninguna

[1] Human-in-the-loop hace referencia a un sistema o proceso en el que un ser humano participa de forma activa en el funcionamiento, la supervisión o la toma de decisiones de un sistema automatizado. En el contexto de la IA, este proceos se refiere a que los seres humanos interfieran en algún momento del flujo de trabajo de la IA con el fin de garantizar la seguridad, responsabilidad y la precisión, en la toma de decisiones éticas (Cole Stryker, 2026).

[2] Proceso estructurado para identificar, evaluar y mitigar los riesgos potenciales, beneficios y consecuencias legales o éticas de los sistemas de inteligencia artificial antes y durante su implementación.

decisión de alto impacto es enteramente automatizada sin revisión humana (ISO 42001:2023 Cláusula 8.6). Verificación: procesos de decisión automatizada y mecanismos de revisión humana.

Nivel 4 - Gestionado: SGIA auditado y XAI plena

El Nivel 4 activa el cuarto eje de la ISO 42001:2023. El SGIA tiene auditoría interna anual con plan de no conformidades reportado a la alta dirección. Los sistemas de IA de alto riesgo tienen documentación XAI[3] completa y verificable. El registro de datos de entrenamiento garantiza que los modelos no fueron entrenados con datos sesgados. La cadena de suministro IA, modelos preentrenados, APIs externas, datasets de terceros, está inventariada y evaluada.

- **I4.IA.1:** El SGIA tiene auditoría interna anual documentada con plan de tratamiento de no conformidades aprobado y reporte formal a la alta dirección (ISO 42001:2023 Cláusula 9.2). Eje 4, Auditoría SGIA. Verificación: informe de auditoría interna del SGIA y plan de tratamiento de no conformidades.
- **I4.IA.2:** Todos los sistemas de IA de alto riesgo tienen documentación de explicabilidad (XAI) completa y verificable: datos de entrenamiento usados, proceso de toma de decisiones, limitaciones del modelo y mecanismos de apelación para los afectados (Anexo A.7 y A.8.4). Eje 1, XAI plena. Verificación: documentación XAI de los sistemas de IA de alto riesgo.
- **I4.IA.3:** Existe registro documentado de los datos de entrenamiento de los modelos de IA usados institucionalmente, con control de calidad (ausencia de sesgos conocidos), trazabilidad de procedencia y mecanismo de actualización periódica (Gobernanza de datos, Anexo A.6.1). Verificación: registro de datos de entrenamiento y proceso de control de calidad.
- **I4.IA.4:** La cadena de suministro de IA —modelos preentrenados utilizados, APIs externas integradas, datasets de terceros, está inventariada y evaluada con criterios de riesgo documentados (Anexo A.9.2). Eje 3, Control de cadena de suministro. Verificación: inventario de cadena de suministro IA y criterios de riesgo aplicados.

[3] Conjunto de procesos y métodos que permite a los usuarios humanos comprender y confiar en los resultados y los productos creados por los algoritmos de machine learning https://www.ibm.com/es-es/think/topics/explainable-ai

Nivel 5 - Resiliente: SGIA certificado y gestión total del ecosistema

El Nivel 5 es el horizonte más ambicioso del modelo: el SGIA está en proceso formal de certificación bajo la ISO 42001:2023 con Statement of Applicability del Anexo A documentado. La política de gobernanza ética de IA está alineada con el EU AI Act para sistemas universitarios de alto riesgo (calificación automatizada, verificación de identidad para exámenes, monitoreo estudiantil). Ciclos de mejora continua semestrales. Vigilancia sobre criptografía post cuántica. Ecosistema IA completamente auditado.

- **I5.IA.1:** El SGIA está en proceso formal de certificación o ya certificado bajo ISO 42001:2023, con Statement of Applicability (SoA) del Anexo A documentado que especifica qué controles aplican, cuáles no aplican y la justificación de las exclusiones, con evidencia de que los controles declarados están implementados y auditados externamente. Verificación: SoA e informe de la última auditoría externa.
- **I5.IA.2:** La política de gobernanza ética de IA está alineada con el (European Commision, 2024) para los sistemas universitarios de alto riesgo: sistemas de evaluación del rendimiento estudiantil, verificación de identidad para exámenes y sistemas de monitoreo del comportamiento estudiantil. Verificación: política de gobernanza de IA y su mapeo con las categorías de alto riesgo del EU AI Act relevantes para el contexto universitario.
- **I5.IA.3:** Los ciclos de mejora continua del SGIA se realizan con periodicidad semestral, con revisión formal de la alta dirección que incluye métricas de rendimiento del sistema de gestión de IA y lecciones aprendidas de incidentes (ISO 42001:2023 Cláusula 10). Verificación: actas de revisión por la dirección del SGIA de los últimos cuatro semestres.
- **I5.IA.4:** Existe plan activo documentado de vigilancia sobre estándares de criptografía post-cuántica (NIST FIPS 203/204/205, publicados en 2024) con evaluación del impacto en la infraestructura de IA institucional y plan de migración con horizonte temporal definido. Verificación: plan de vigilancia sobre PQC[4] y evaluación de impacto.

[4] PQC Post-Quantum Cryptography. En español: Criptografía Post Cuántica.

- I5.IA.5: El ecosistema IA completo, modelos propios, APIs externas, datos de entrenamiento, proveedores, cadena de suministro, está inventariado, evaluado con criterios de riesgo documentados, controlado mediante contratos con cláusulas de auditoría y auditado externamente al menos una vez por año. Verificación: informe de auditoría anual del ecosistema IA.

7.3. Indicadores - Dimensión Seguridad de IA

Ilustración 7.
Indicadores - Dimensión Seguridad de IA

Nota. Ilustración 7. Indicadores de la Dimensión Seguridad de IA (D5-IA). 20 indicadores totales — mayor número de todas las dimensiones. Dimensión diferenciadora: ningún modelo previo la incorpora como dimensión autónoma. Sus 20 indicadores integran los cuatro ejes de la ISO/IEC 42001:2023. Elaboración propia.

8. CULTURA ORGANIZACIONAL DE SEGURIDAD: VARIABLE MODERADORA TRANSVERSAL

Tipo: Variable moderadora transversal · **Presencia:** Todos los niveles como condición de sostenibilidad

Respaldo: Hallazgo H2 de la investigación, cuatro de cinco instrumentos identifican la cultura como causa raíz del déficit de madurez

8.1. Función Moderadora en el Modelo

La Cultura Organizacional de Seguridad no es una sexta dimensión sino una variable moderadora transversal: opera como condición de sostenibilidad de los niveles alcanzados en las otras cinco dimensiones. Una institución puede tener todos los indicadores del Nivel 4 formalmente implementados (CISO, política actualizada, SIEM, SOC, metodología de riesgos) pero si no existe una cultura que haga que el personal reporte incidentes voluntariamente, que los docentes adopten buenas prácticas sin imposición y que los estudiantes comprendan su rol en la seguridad institucional, el Nivel 4 es frágil y retrocedería ante la rotación de personal o la reducción presupuestal.

El Hallazgo H2 del OE2 sustenta esta concepción: cuatro de los cinco instrumentos identifican la cultura como causa raíz del déficit de madurez, no como consecuencia. El personal TI de la UNAD lo formuló en las respuestas abiertas del Instrumento 2: "condición fundacional — sin ella, cualquier inversión tecnológica queda incompleta." Esta cita directa es la única que el modelo incorpora explícitamente, dado su carácter paradigmático para entender la relación entre cultura y madurez técnica.

8.2. Criterios de Cultura por Nivel

Nivel 1 Reactivo: No existe concienciación institucional. La seguridad es responsabilidad exclusiva de TI sin participación de la comunidad. Los incidentes se ocultan por temor a consecuencias. No se realizan campañas de sensibilización.

Nivel 2 Emergente: Campañas esporádicas de concienciación sin medición de impacto ni cobertura sistemática. La dirección reconoce la importancia de la ciberseguridad pero no la promueve activamente. Los incidentes se reportan solo cuando son inevitables.

Nivel 3 Estructurado: Programa anual de concienciación con cobertura documentada de toda la comunidad universitaria (docentes, estudiantes, personal administrativo) y evaluación básica de resultados.

Nivel 4 Gestionado: La cultura de seguridad se mide con indicadores de comportamiento. El reporte voluntario de incidentes está institucionalizado y explícitamente no penalizado. La alta dirección comunica activamente el compromiso institucional con la ciberseguridad.

Nivel 5 Resiliente: La cultura de seguridad es parte de la identidad institucional. Los simulacros de phishing, los ejercicios de concienciación y las actualizaciones sobre amenazas emergentes forman parte del calendario académico y administrativo permanente. La comunidad comprende y asume activamente su rol en la resiliencia digital.

9. POSICIONAMIENTO DIAGNÓSTICO DE LA UNAD EN EL MODELO MMCC-IES

El diagnóstico piloto de la UNAD (Instrumento 2, n=14, personal TI y ciberseguridad, marzo-mayo 2026) provee el primer posicionamiento empírico de una IES colombiana en el modelo MMCC-IES. Este posicionamiento es diferenciado por dimensión, lo que permite identificar el perfil específico de fortalezas y brechas en lugar de un nivel global homogéneo.

Tabla 2.
Posicionamiento de la UNAD respecto al modelo MMCC-IES

Dimensión	Nivel diagnosticado	Confianza diagnóstica	Fortalezas principales	Brechas específicas hacia el siguiente nivel
D1: Gobernanza	N3 - N4 (transición)	Alta	Apoyo directivo (78,6%). Políticas formales (64,3%).	Integrar ciberseguridad en PDI con metas medibles. Tablero de KPIs mensual. Reportes formales al Consejo Superior.
D2: Talento Humano	N3 consolidado	Muy alta	Estructura REDSIIUNAD formalizada. Articulación ECBTI-CSIRT. Nivel técnico alto (85,7%).	Plan de certificación con presupuesto. Evaluación formal de brechas K-S-A. Formalización del perfil de especialista IA.
D3: Gestión de Riesgos	N3 en proceso	Media	Tiempos de validación REDSIIUNAD formalizados. Evaluaciones de vulnerabilidades realizadas.	Metodología formal de evaluación de riesgos con ciclo anual completo. Análisis de riesgos como condición formal para proyectos TI.
D4: Cap. Técnicas	N3 parcial	Alta	SIEM operativo (50%). Continuidad operativa (50%). Gestión de accesos activa.	SIEM al 100% de sistemas críticos. SOC con monitoreo 24/7. BCP/DRP formalmente probado con RTO/RPO. Hardening sistemático CIS.
D5: Seguridad IA	N1 - N2 (urgente)	Muy alta	VIEM activa en adopción tecnologías emergentes. CSIRT consciente del problema.	PRIORITARIO: Aprobar política básica de IA. Inventario inicial con Shadow AI. Primer AIIA. Primera evaluación de sesgos. Cláusulas de auditoría en contratos IA.

Cultura Organizacional	N2 - N3 (transición)	Media	Conciencia del equipo técnico sobre la importancia de la cultura. Formación esporádica realizada.	Programa anual de concienciación con cobertura institucional completa. Institucionalizar el reporte voluntario de incidentes sin penalización.

Nota. Tabla 2. Posicionamiento diagnóstico de la UNAD en el Modelo MMCC-IES por dimensión, con fortalezas y brechas específicas. La confianza diagnóstica refleja la solidez de la evidencia empírica disponible del OE2 para cada dimensión. Fuente: Instrumento 2 (n=14, personal TI UNAD, 2026). Elaboración propia.

El posicionamiento revela que la paradoja técnico-gobernanza se reproduce a nivel de dimensiones: las fortalezas más consolidadas están en Talento Humano (N3 consolidado) y Gobernanza (N3 con algunas capacidades de N4), mientras que la brecha más urgente está en Seguridad de IA (N1-N2), donde el 93% del personal confirma la ausencia de lineamientos. Esta distribución es representativa del perfil diagnóstico de las IES colombianas más avanzadas: inversión en talento técnico y estructuras de gobernanza sin gestión de los riesgos específicos de IA.

La ruta prioritaria para la UNAD es simultánea: Ruta 3-4 en las dimensiones de Gobernanza, Gestión de Riesgos y Capacidades Técnicas (horizonte 12 - 24 meses), y Ruta 1-2 con urgencia en la Dimensión de Seguridad de IA (horizonte 0 - 12 meses). El objetivo de corto plazo más crítico es avanzar desde la opacidad total hasta tener política básica de IA, inventario inicial y primer AIIA.

10. RUTAS EVOLUTIVAS INSTITUCIONALES ESCALABLES

Las rutas evolutivas son el cuarto componente y la concreción práctica: "proponer rutas de mejora institucional escalables". Cada ruta describe la transición entre dos niveles consecutivos con acciones prioritarias diferenciadas por dimensión, horizonte temporal estimado y criterios de avance verificables. Son escalables: aplican a cualquier IES colombiana independientemente de su tamaño, modelo de operación o nivel de recursos.

Tabla 3.
Rutas evolutivas institucionales

Ruta	Horizonte	Acciones prioritarias diferenciadas por dimensión	Criterio verificable de avance	Señal de alerta — riesgo de implementación formal sin sustancia
1-2	0 - 12 meses	GOB: aprobar política de ciberseguridad y política de uso aceptable de IA. Designar responsable con mandato. Asignar presupuesto básico. TAL: identificar funciones básicas de seguridad. Enviar al menos un integrante a certificación básica. RIE: construir inventario básico de activos e inventario inicial de sistemas IA con Shadow AI identificado. TEC: implementar firewall, AV, backups verificados y control básico de accesos con mínimo privilegio. IA: documentar descripción básica de algoritmos de alto impacto (Transparencia inicial A.8.2).	Política ciberseguridad aprobada · Responsable designado · Inventario activos e inventario IA documentados · Controles perimetrales operativos.	Política aprobada pero sin presupuesto real. Responsable designado sin tiempo dedicado. Inventario incompleto o sin actualización.
2-3	6 - 18 meses	GOB: formalizar CISO con KPIs y acceso directivo. Alinear política con ISO 27001:2022. TAL: estructurar dos equipos diferenciados con perfiles NICE/ECSF. Articular con programas académicos. RIE: aplicar metodología formal de evaluación de riesgos con ciclo anual. TEC: implementar SIEM y MFA en sistemas críticos. Probar plan IR mediante simulacro. IA: realizar primer AIIA. Primera evaluación de sesgos. Incluir cláusulas de transparencia y auditoría en contratos IA.	SIEM operativo · MFA activo · Dos equipos diferenciados · AIIA documentado · Evaluación de sesgos realizada · Contratos IA con cláusulas de auditoría.	CISO sin acceso real al comité directivo. SIEM instalado pero no monitoreado activamente. AIIA realizado pro forma sin impacto en decisión.

3-4	12 - 24 meses	GOB: integrar ciberseguridad en PDI con metas medibles y presupuesto propio. TAL: plan de certificación anual con presupuesto. Evaluar brechas K-S-A por rol. RIE: hacer análisis de riesgos condición para proyectos TI. Implementar tiempos de validación REDSIIUNAD. TEC: establecer SOC 24/7. Documentar y probar BCP/DRP. Implementar hardening CIS Benchmarks. IA: auditoría interna anual del SGIA. XAI completa para sistemas de alto riesgo. Inventariar cadena de suministro IA.	Ciberseg. en PDI · SOC operativo con métricas · BCP/DRP probado · Auditoría SGIA anual · XAI completa para sistemas críticos.	Ciberseguridad en PDI sin presupuesto real. SOC contratado pero sin revisión mensual de métricas. Auditoría SGIA formal sin plan de remediación.
4-5	18 - 36 meses	GOB: alinear gobernanza de IA con EU AI Act. Iniciar proceso de certificación ISO 42001:2023. TAL: formalizar perfil de especialista IA. Incorporarse a redes CSIRT internacionales. RIE: implementar programa de threat intelligence trimestral con Analista de Ciberamenazas. TEC: implementar XDR/MDR con ML. Desplegar arquitectura Zero Trust. Programa trimestral de threat hunting proactivo. IA: obtener o avanzar en certificación ISO 42001. Activar plan de vigilancia PQC. Auditar ecosistema IA completo.	XDR/MDR con ML · Zero Trust en segmentos críticos · Proceso ISO 42001 iniciado · Gobernanza ética IA con EU AI Act · Threat hunting trimestral con informes.	XDR implementado solo con reglas estáticas sin ML real. Zero Trust declarado sin verificación continua de dispositivos. ISO 42001 en proceso sin evidencia de avance.

Nota. Tabla 3. Rutas evolutivas institucionales del MMCC-IES. Las señales de alerta identifican las implementaciones formales sin sustancia real más frecuentes, un riesgo documentado en los modelos de madurez cuando se usan con fines de imagen institucional en lugar de mejora real. Elaboración propia.

11. REFERENCIAS BIBLIOGRÁFICAS

Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science*, *7*, e703. https://doi.org/10.7717/peerj-cs.703

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

CIS. (2021). *CIS Control v8*. https://www.cisecurity.org/controls/v8

Cole Stryker. (2026). *¿Qué es human-in-the-loop?* https://www.ibm.com/es-es/think/topics/human-in-the-loop

ENISA. (2022). *EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)*. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf

European Commision. (2024). *The EU Artificial Intelligence Act*. https://artificialintelligenceact.eu/

(Gcscc), G. C. S. C. C. (2021). Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3822153

Harun Or Rashid, Md., & Mustafa, H. A. (2026). Adoption of Zero Trust Architecture in Higher Education Institutions in Bangladesh (ZTA-HEIs): Strategies, challenges, and readiness. *Journal of King Saud University Computer and Information Sciences*. https://doi.org/10.1007/s44443-026-00618-5

ISC2. (2024). *2025 ISC2 Cybersecurity Workforce Study*. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

ISO. (2023). *ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system*. https://www.iso.org/standard/42001

MinTIC. (2025). *Modelo de Seguridad y Privacidad de la Información—MSPI*. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Murphy, D., Tryfona, N., & Marshall, A. (2023). *A Targeted Study on the Match between Cybersecurity Higher Education Offerings and Workforce Needs*. https://doi.org/10.25778/JX3E-6785

National Institute of Standards and Technology. (2024a). *NIST Cybersecurity Framework 2.0: Cybersecurity Supply Chain Risk Management (C-SCRM) Quick-Start Guide* (NIST SP 1305 ipd; p. NIST SP 1305 ipd). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1305.ipd

National Institute of Standards and Technology. (2024b). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology (US). (2024). *Stateless hash-based digital signature standard* (NIST FIPS 205; p. NIST FIPS 205). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.FIPS.205

NIST. (2020). *NIST SP 800-181 Rev. 1 Workforce Framework for Cybersecurity (NICE Framework)*. https://csrc-nist-gov.translate.goog/pubs/sp/800/181/r1/final?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1

REDSIIUNAD. (2025). *RESOLUCIÓN No. 009016 DEL22 DE MAYO de 2025*. https://csirt.unad.edu.co/images/2025/Resolucion%20REDSIIUNAD.pdf

Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in Higher Education Institutions Digitalisation: Addressing Threats and Vulnerabilities. *Sage Open*, *16*(1), 21582440251413473. https://doi.org/10.1177/21582440251413473

Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1; p. NIST AI 100-1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.AI.100-1

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z